Implementación de web application firewall basado en servicios Cloud e IoT

Autores

Jesus Eduardo Ramos Guzmán
Juan Carlos González
Miguel Ángel Bejarano

Directores:
Ing. Mónica Espinosa Buitrago PhD
Ing. Elvis Eduardo Gaona García PhD

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
ESPECIALIZACIÓN EN GESTIÓN DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN
BOGOTÁ, 2023

Dedicatoria

A nuestros familiares y amigos que creyeron en nosotros, por su colaboración y dedicación cada día para seguir adelante con nuestros sueños.

Agradecemos a la Universidad Santo Tomas ya que sin el desarrollo de la especialización en gestión de servicios de tecnologías de la información no sería posible la adquisición del conocimiento en cada uno de nosotros como profesionales íntegros en el desarrollo tecnológico de las nuevas tecnologías.

AGRADECIMIENTOS

Agradecimientos a la Universidad Santo Tomás por permitirnos brindar nuestros conocimientos aplicados a las nuevas tecnologías.

Agradecemos a los docentes que hicieron parte de este camino, por guiarnos y enseñarnos sus conocimientos en las diversas ramas profesionales, recordándonos cada día la importancia de conservar las ganas de aprender todos los días con la convicción de ser mejores personas y profesionales cada día.

Tabla de Contenido

ACRÓNIMOS

Acrónimo	Definición
WAF	Cortafuegos de aplicaciones web
AWS	Servicios web de Amazon
IoT	Internet de las cosas
MiPymes	Micro, pequeña o mediana empresa
WEB	World Wide Web
DMZ	Zona desmilitarizada
TIC	Tecnología de la información y la comunicación
SQL	Lenguaje de consulta estructurado
XSS	Scripts entre sitios
OSI	Sistemas abiertos de interconexión
TI	Tecnologías de la Información
CIIU	Clasificación Industrial Internacional Uniforme
UIT	Unión Internacional de Telecomunicaciones
GCI	Índice de Ciberseguridad Global
NCSI	National Cyber Security Index
HTPPS/HTPP	Protocolo de transferencia de textos seguros / protocolo de transferencia de textos
FTPS/FTP	Protocolo de transferencia de archivos seguros / Protocolo de transferencia de archivo
ACOPI	Asociación Colombiana de las Micro, Pequeñas y Medianas Empresas
AZ	Zonas de disponibilidad
API	Interfaz de programación de aplicaciones

RESUMEN

La presente monografía tiene como objetivo la presentación de una propuesta de asesoría para la implementación de WAF con AWS es un servicio que ofrece la empresa para ayudar a los clientes a proteger sus aplicaciones web de ataques maliciosos.
El objetivo es brindar una solución personalizada y de calidad que garantice la seguridad y el rendimiento de las aplicaciones web de los clientes.

El WAF(web application firewall) es una herramienta que filtra y bloquea el tráfico no deseado y potencialmente dañino que intenta acceder a las aplicaciones web. El AWS (Amazon Web Services) es una plataforma de servicios en la nube que permite alojar y gestionar las aplicaciones web de forma segura y eficiente. Nuestra asesoría consiste en los siguientes pasos:

- Análisis de las necesidades y requisitos del cliente.
- Diseño de la arquitectura y la configuración del WAF y el AWS.
- Implementación y prueba del WAF y el AWS.
- Capacitación y soporte al cliente.

En una época donde la mayoría de los negocios están en línea, la seguridad de la aplicación web es vital para proteger la información del cliente y mantener una sólida reputación. Con una implementación adecuada del WAF, los usuarios pueden disfrutar de un alto nivel de seguridad en su aplicación web, lo que a su vez aumenta la confianza del cliente y ayuda a la empresa a avanzar en su negocio. En resumen, es una herramienta imprescindible para cualquier organización que busque proteger su aplicación web contra futuras amenazas.

ABSTRACT

The purpose of this monograph is to make an advisory proposal for the implementation of waf with aws is a service offered by the company to help customers protect their web applications from malicious attacks.
The objective is to provide a personalized and quality solution that guarantees the security and performance of clients' web applications.

The waf (web application firewall) is a tool that filters and blocks unwanted and dangerous traffic trying to access web applications. The aws (Amazon Web Services) is a cloud service platform that allows you to host and manage web applications safely and efficiently. Our advice consists of the following steps:

- Analysis of customer needs and requirements.
- Design of the architecture and the configuration of the waf and the aws.
- Implementation and testing of waf and aws.
- Training and customer support.

In an age where most businesses are online, web application security is vital to protecting customer information and a strong reputation. With a proper implementation of the WAF, users can enjoy a high level of security in their web application, which in turn increases customer trust and helps the company to advance its business. In short, it is a must have tool for any organization looking to protect their web application against future threats.

INTRODUCCIÓN

Gracias a la globalización, los avances tecnológicos se han incrementado de manera constante, en este panorama los datos y la información se convierten en los activos más preciados de todas las compañías sin importar el sector económico en el que se desempeñen. En este contexto las empresas deben adaptarse, digitalizar sus activos informáticos aumentando así el uso de aplicaciones tecnológicas en las que intervienen diferentes actores como lo son equipos de cómputo, infraestructura de red, personas y por supuesto conexiones a internet. Debido a la hiperconectividad que existe en la actualidad, los ataques cibernéticos son cada vez más frecuentes en el mundo según cifras de la CCIT (Cámara Colombiana de Informática y Telecomunicaciones); el acceso sin autorización a sistemas informáticos presentó 6.407 casos en el año 2022 y el hurto por medios Informáticos presentó un aumento del 15% con respecto al año 2021 con más de 11.078 casos [1]. Lo que tiene graves consecuencias en las economías de las empresas y los países que son atacados, ya que en la mayoría de estos ataques la única posibilidad de recuperar los datos perdidos es accediendo a pagar grandes sumas de dinero, esto sin contar las innumerables fraudes que a diario sufren las personas del común donde ven cómo sus cuentas bancarias son vaciadas, sus redes sociales son secuestradas o como su información personal e íntima son expuestas si no acceden a cancelar sumas de dinero a los Ciber delincuentes.

La ausencia de inversión en temas de seguridad como también la falta de información necesaria, oportuna y concreta son algunos de los motivos por los cuales no se cuenta con políticas de seguridad y protección eficientes en las empresas. Debido a esto, en la siguiente monografía se pretende realizar un análisis de las circunstancias actuales de la seguridad informática involucrando también temas de Cloud e IoT, para poder ofrecer servicios de consultoría implementando una solución WAF para proteger los servicios Cloud e IoT que ofrecen empresas MiPymes a nivel nacional que no cuentan con un sistema de seguridad web, para así proteger sus servicios de ataques a sus aplicaciones web.

1. PROBLEMA

1.1. ÁRBOL DE PROBLEMAS

La problemática surge de la necesidad de proteger datos sensibles para cualquier compañía, teniendo en cuenta que los servicios Cloud (computación en la nube) son la forma directa para acercarse a los activos más valiosos para una compañía como lo son los datos, convirtiéndolos en objetivos fáciles para los hackers o personas mal intencionadas. Por esto se genera la necesidad de plantear una capa extra de seguridad en la DMZ (zona desmilitarizada), para la protección contra ataques dirigidos o de alta complejidad técnica.

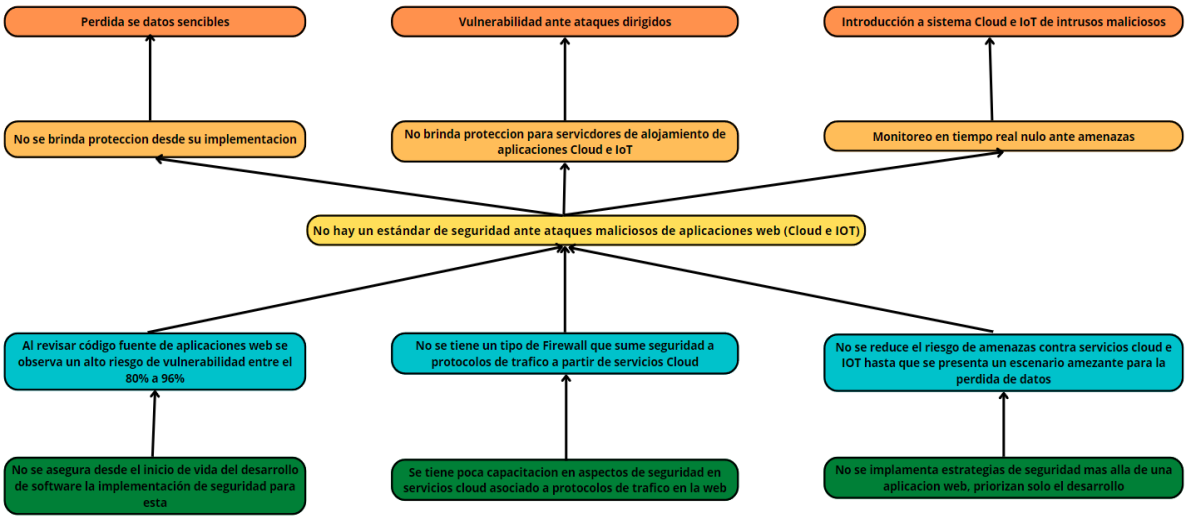

Figura 1 Árbol de problemas

1.2. QUÉ SE QUIERE SOLUCIONAR

En el mundo actual se observa que existe cada vez más conectividad, el internet de las cosas (IoT, por sus siglas en inglés) donde se ofrecen nuevos servicios a nivel personal y comercial en todo el mundo, el punto central de esto es la creación y el intercambio de datos, que nos brinda nuevas formas de vivir y trabajar. Pero, se necesita tener confianza para que los objetos conectados y los datos que se generan solo sean observados y analizados por las personas correctas.

En los últimos años, los servicios web y dispositivos inteligentes han recopilado datos a niveles alarmantes, lo que genera preocupación en el sector de las TIC (tecnología de la información y la comunicación) ya que se ha vuelto uno de los principales retos del sector, para garantizar la integridad de los datos ante vulnerabilidades existentes en Cloud e IoT.

Debemos tener en cuenta que, uno de los principales consumidores de estas tecnologías son las grandes, pequeñas y medianas empresas, pero sabemos que los actores más vulnerables a ataques en sus redes son las empresas medianas y pequeñas, por falta de recursos y poca capacitación en temas de seguridad a nivel de Cloud e IoT. [2]

El ataque más común sobre las aplicaciones web es la inyección SQL, la cual se diseñó con el fin de aprovechar errores en la programación. Teniendo en cuenta que es un lenguaje de programación con acceso a base de datos, siempre están vulnerables los datos de las compañías.

Como los dispositivos y las redes implementadas no cuentan siempre con las medidas de seguridad mínimas, se convierten en objetivos vulnerables para los hackers, como sucede en los teléfonos móviles, aplicaciones y computadoras. Ya que son objetivos muy fáciles de atacar, los hackers cada vez más desarrollan software de alto nivel, con el único objetivo de robar información (datos) a partir de los servicios Cloud e IoT por su alta vulnerabilidad.

Para poder contraatacar estas vulnerabilidades existentes a nivel de Cloud e IoT, se implementará un **Firewall de Aplicaciones Web** (WAF) para ayudar a proteger aplicaciones WEB, a partir de un filtrado de protocolos, mejorando en tiempo real las reacciones de posibles ataques a nuestras aplicaciones y con el objetivo de controlar posibles falsificaciones de sitios, scripts entre sitios XSS, inyecciones de código y muchos más escenarios existentes. WAF es una defensa que pertenece a la capa 7 del modelo OSI y está diseñado para la mitigación de ataques a partir de un paquete de herramientas, para crear así una defensa integral para las compañías.

2. IDEACIÓN DE LA SOLUCIÓN

En la actualidad, se observa un crecimiento acelerado de aplicaciones web y servicios de IoT a nivel mundial. Al ser consumidas por tantos usuarios, están más disponibles para sufrir ataques, la idea de crear aplicaciones y servicios es hacerlas tolerantes a vulnerabilidades y fallos, por diferentes aspectos de seguridad no siempre es así.

Se pretende implementar el servicio de WAF para proteger los servicios Cloud e IoT que ofrecen empresas MiPymes a nivel nacional que no cuentan con un sistema de seguridad web, para así proteger sus servicios de ataques al servidor de aplicaciones web y garantizar la seguridad mediante análisis de paquetes y peticiones de diversos protocolos y modelos de tráfico.

Al implementar WAF, se obtiene una mejor administración de recursos ya que se centraliza la gestión de amenazas en un solo punto y así mitigar ataques conocidos y ataque nuevos de una forma automatizada. [3]

2.1 POR QUÉ SE PLANTEA AHORA LA SOLUCIÓN

La creciente demanda de aplicaciones WEB de las compañías a nivel nacional para poder mantenerse en el mercado y así poder soportar sus servicios ante los clientes. La criticidad del tema aparece cuando al momento de evaluar la seguridad que usan las compañías para garantizar la disponibilidad e integridad de la información ya que la mayoría usan la internet.

Los ataques normalmente aprovechan las vulnerabilidades de seguridad para redireccionar sitios web a direcciones falsas para así poder robar información sensible [4], las condiciones de seguridad a nivel nacional para las empresas pymes son muy vulnerables, la necesidad surge a nivel de la sensibilidad de datos que se maneja y que esto también podría afectar económicamente y judicialmente a las compañías este servicio se prestaría a este sector ya que son los que no estarían capacitados e informados de los riesgos a los que se enfrentan si no se tiene en cuenta la seguridad de sus aplicaciones WEB.

2.2 SECTOR OBJETIVO

La seguridad informática es primordial para todas las empresas que utilizan aplicaciones o software para el manejo de sus diferentes datos de gestión, de

históricos, de transacciones entre otros. Acoger políticas de seguridad informática es imperativo para la permanencia de las empresas sin importar el tipo de negocio o el tamaño. El sector de Software y TI cómo se categoriza en Colombia Productiva, se identifica por su capacidad de revolucionar, fomentar y transmitir tecnología a todas las comunidades económicas. También cuenta con una fuerza de crecimiento y generación de empleos.

Nuestra solución va orientada a las empresas de diferentes sectores económicos como la agroindustria, manufacturas y servicios a través de una consultoría y una aplicación tecnológica para proteger todas las capas de sus aplicaciones de funcionamiento interno.

Nuestro sector objetivo se encuentra dentro de la categoría de servicios, el sector de Software y TI. Este sector cuenta con gran probabilidad de crecimiento ya que todo apunta a que se posicione como el pilar más importante para la capacidad de hacer las cosas mejor de las empresas proporcionando soluciones que favorecen la venta de productos, el contacto con clientes y proveedores. La comunicación de información estratégica contribuye a la toma de decisiones, entre otras utilidades. [5]

Las tendencias a nivel local y mundial en este sector se orientan en soluciones en internet, aplicaciones móviles, análisis, tratamiento de datos y aplicaciones empresariales. De igual forma, según la visión que se plantea en Colombia Productiva se quiere obtener un aumento en los beneficios percibidos de los servicios asociados con el desarrollo de Software y Tecnologías de la Información. Promover y centrarse en segmentos específicos de la industria, con la finalidad de focalizar el trabajo de educación, investigación y desarrollo, política pública, e infraestructura estatal. Se entiende que con esta visión se quiere llevar al sector de Software y TI a un nivel más especializado en las diferentes tecnologías y para lograr esto se deben articular diferentes organizaciones en pro de un mismo objetivo.

Se tiene como propósito aumentar en 10% la intervención de compañías con servicios y productos propios; así como un incremento de un 15% en las ventas a otros países frente a las ventas totales. Para lograr esta meta propuesta, es primordial la conformación de profesionales mucho más capacitados no solo en temas de TI sino que también con dominio de una lengua extranjera, logrando así desarrollar ofertas cada vez más especializadas apropiándose del uso de tecnologías de última generación.

Este sector es un generador de valor agregado para la mayoría de los sectores productivos en Colombia dejando huella directa en la situación financiera tanto de las

regiones como locales mejorando así temas como calidad de vida para sus pobladores, desigualdades sociales. Contribuyendo la cooperación de la comunidad en diferentes redes que les da la oportunidad de enfrentar los problemas reduciendo las condiciones de desigualdad. [6]

Según las cifras mostradas por Colombia Productiva, sus principales datos económicos son:

- Entre enero y junio del 2019 las rentas representativas de la industria se ampliaron en 13,9%, comparados con los primeros seis meses de 2018.
- La ocupación total de los primeros seis meses de 2019 aumentó en 11,3%, comparado con el primer semestre de 2018.
- Las ventas de productos o servicios a otros países del sector se mermaron en 4,9% durante el primer semestre de 2019.En esta misma vía el segmento de servicios de informática se redujo en 0,3% así como el de licencias para reproducir en 26,2%. [7]

En la siguiente tabla se muestran las actividades ejercidas por el sector Software Y TI en Colombia. [8]

Desarrollo de sistemas informáticos consultoría informática y actividades relacionadas.	
Código CIIUU	Actividad Economica
620	Desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas), consultoría informática y actividades relacionadas
6201	Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño,
6202	Actividades de consultoría informática y actividades de administración de
6209	Otras actividades de tecnologías de información y actividades de servicios
División 63. Actividades de servicios de información	
Código CIIUU	Actividad Economica
631	Procesamiento de datos, alojamiento (hosting) y actividades relacionadas;portales web.
6311	Procesamiento de datos, alojamiento (hosting) y actividades relacionadas.
6312	Portales web.
639	Otras actividades de servicio de información.
6391	Actividades de agencias de noticias.
6399	Otras actividades de servicios de información n.c.p.

Tabla 1. Actividades económicas desarrolladas por el sector Fuente DIAN

La solución planteada según esta clasificación está incluida en el código CIIU (Clasificación Industrial Internacional Uniforme) 6202.

2.3 TENDENCIAS DEL SECTOR

Las tendencias internacionales según la Unión Internacional de Telecomunicaciones por sus siglas en inglés UIT estiman que aproximadamente 5300 millones de

personas, o el 66% de la población mundial, utilizará Internet en 2022. Esto representa un aumento del 24% desde 2019 y se estima que 1100 millones de personas se conectaron durante ese período. Sin embargo, esto deja a 2.700 millones de personas aún fuera de línea. [9]

Esto muestra el crecimiento acelerado de conexiones a internet esto evidencia que cada vez más personas en el mundo utilizan este medio para realizar diferentes actividades, transacciones y consultas jugando un papel fundamental la seguridad informática.

La ciberseguridad se ha convertido en un factor primordial, dado que más sectores productivos a nivel mundial utilizan cada vez más aplicaciones web para el tratamiento de sus datos. En vista de estos la UIT lanzó en el 2015 el Índice de Ciberseguridad Global por sus siglas en inglés (GCI) formada y mejorada por el trabajo de una amplia gama de expertos y colaboradores dentro de los países y otras organizaciones internacionales.

Los resultados del GCI muestran una mejora general y el fortalecimiento de los pilares de la agenda de seguridad cibernética, pero persisten las brechas regionales en la capacidad cibernética. En el informe se han destacado prácticas ilustrativas de los países.

Cada vez es más importante la formación de profesionales enfocados a los diferentes niveles de cibernética a nivel mundial, más del 50 por ciento de los países carecen de programas adaptados a sectores o profesiones específicas, como la aplicación de la ley, los actores legales, PYMES, empresas privadas y funcionarios gubernamentales.[10]

En la siguiente figura se visualiza el Número de países que implementan cursos de ciberseguridad en los planes de estudio nacionales.

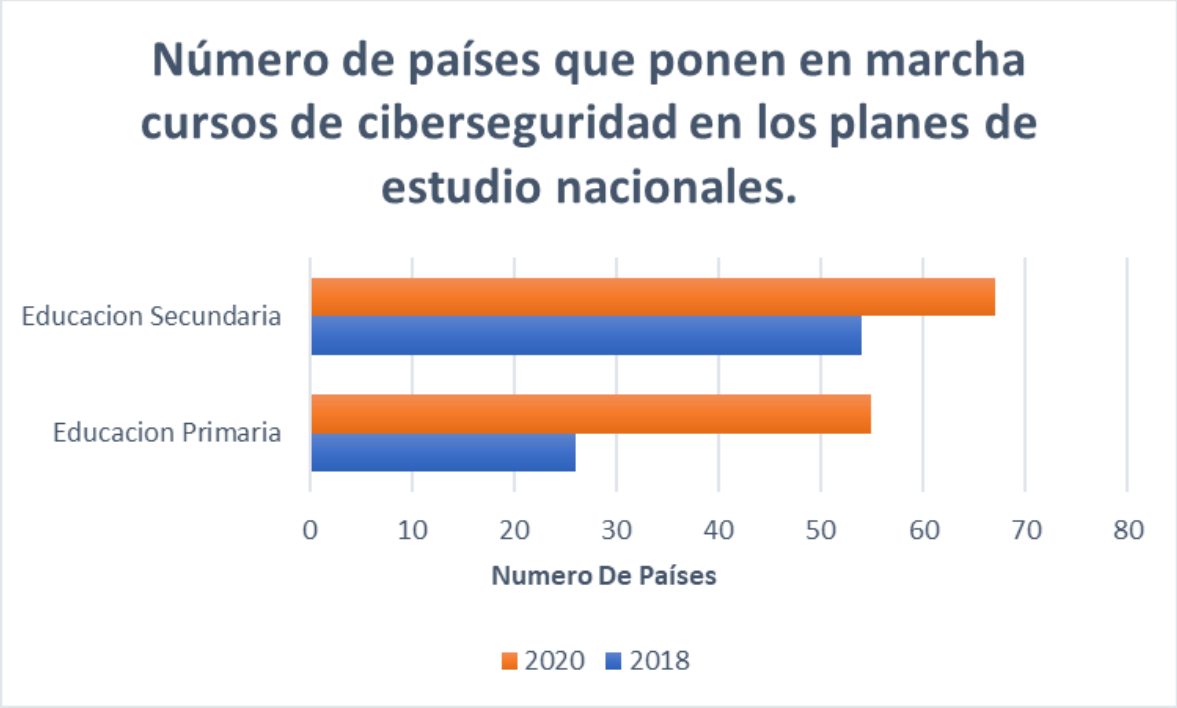

Figura 2. Número de países que implementan cursos de ciberseguridad en los planes de estudio nacionales. Fuente UIT

Por otra parte, los ataques cibernéticos crecen cada día más a nivel Mundial afectando progresivamente a los diferentes sectores productivos de diferentes países. Según unas predicciones realizadas por la página especializada en Seguridad Informática cybersecurityventures.com se espera que los valores asociados a los Ciberataques aumenten en un 15% cada año durante los siguientes 5 años. Se tiene estimado que para 2025 se superen los 10.5 Billones de dólares por año esto con respecto a los 3 Billones de dólares del año 2015 [11].

2.4 ANÁLISIS DE MERCADO

El crecimiento exponencial de la digitalización de los diferentes sectores productivos ha causado que la cantidad de datos y transacciones que se hacen en línea aumente considerablemente según datos de la ANDI (Asociación Nacional de Empresarios de Colombia); luego del inicio de la Pandemia el 60% de las empresas implementan estrategias de transformación digital.[12]

Todo esto sumado a la gran cantidad de vulnerabilidades existentes en la actualidad, hacen que muchos de los servicios ofrecidos a través de aplicaciones web estén

expuestos a diferentes amenazas y ataques generando así pérdidas de información, indisponibilidad en los servicios ofrecidos además de las pérdidas económicas que esto conlleva. Se conocen reportes de la National Cyber Security Index por sus siglas en inglés (NCSI),que indican que Colombia se encuentra en el puesto 65 de la clasificación a nivel mundial de países a nivel de seguridad informática, en temas como prevención de amenazas, respuesta a ataques, y capacidad de respuesta de incidentes y delitos informáticos a una escala mayor[13].Colombia es un mercado en constante crecimiento en cual se tiene contemplado que las empresas destinen muchos más recursos para mejorar su infraestructura de Ciberseguridad, así mismo el presupuesto de las compañías para el año 2021 en materia de seguridad informática fue de alrededor 329 millones de dólares, este crecimiento hace que existan diferentes ofertas y propuestas en el mercado para que las compañías protejan sus datos pero esto muchas veces tienen un costo muy elevado haciendo que las pymes o Microempresas que no cuenten con recursos amplios no puedan acceder a estos servicios, según datos de la Cámara de Comercio de Bogotá solo en Bogotá y en los 59 municipios que están bajo la jurisdicción de dicha Cámara de Comercio en Enero del 2023 hay 12.879 microempresas que renovaron su registro ante dicha entidad este número es un 23% más de los registrado para enero del 2022, igualmente las pymes representan el 99,3% de las empresas con su registro mercantil renovado.[14]

Nuestra solución pretende acompañar, asesorar a estas empresas que no cuentan con grandes recursos económicos y áreas especializadas en Ciberseguridad a través de la tecnología WAF de Amazon Web Services a proteger sus aplicaciones web de manera segura y accesible para todas ellas.

2.5 ÁRBOL DE OBJETIVOS

El árbol de objetivos surge con el fin de resolver lo planteado anteriormente en el árbol de problemas identificando el objetivo general y mencionando las acciones que hacen posible llegar a dicho objetivo, en él se plasma de una manera general esas acciones que llevarán a ofrecer un valor agregado en esta labor de consultoría para nuestro clientes haciendo enfoque en reducir las brechas de seguridad de aplicaciones cloud e IoT ya que es un tema que está en auge y como todo tema ligado a lo tecnológico no está exento de ciberataques que busquen afectar el activo más valioso de una organización, La Información.

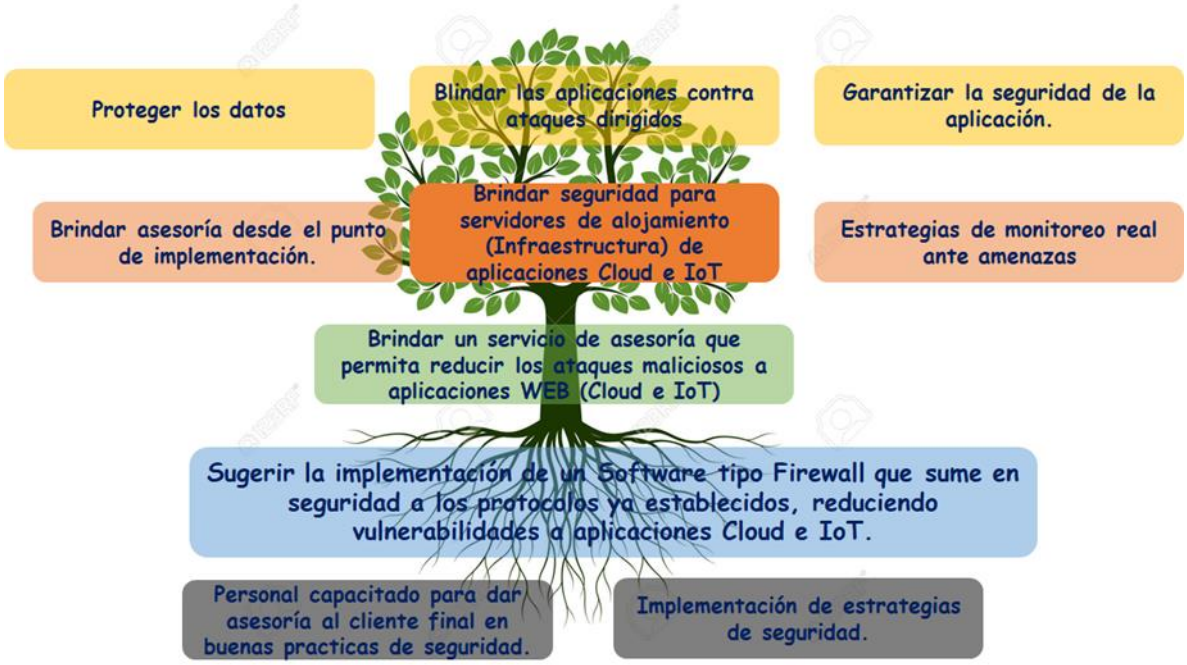

Figura 3. Árbol de objetivos Fuente propia

2.6 CUÁL ES LA SITUACIÓN DESEADA

Con la implementación de un sistema WAF se desea complementar la seguridad de las herramientas en la nube, se profundizará más en las herramientas con un entorno Cloud e IoT.

Al implementar WAF trabajaríamos en un modo llamado Reverse-Proxy (proxy inverso) diríamos que el tráfico que proviene de internet que tiene como objetivo llegar a servicio de cliente, sea analizado en la nube con ayuda de WAF, está realizaría el control de seguridad sobre la capa 7 del modelo OSI (Modelo de interconexión de sistemas abiertos) que sería la capa de aplicación, creando peticiones a los servidores públicos a través de sesiones seguras, debemos tener en cuenta que esta plataforma trabaja bajo la protección de aplicaciones con protocolos de seguridad HTPPS/HTPP (protocolo de transferencia de textos seguros / protocolo de transferencia de textos) FTPS/FTP (Protocolo de transferencia de archivos seguros / Protocolo de transferencia de archivos) y Servicios web, directamente enfocados en la capa de transporte, buscando garantizar protección efectiva y adecuada de los datos.

Se presenta la figura de modelo OSI – WAF donde se muestra la capa 7 perteneciente a la capa de aplicación, ya que es la que muestra la información al usuario final.

Figura 4. Modelo OSI – WAF Fuente Propia.

Teniendo en cuenta que WAF es una tecnología de blindaje para los datos, no se requiere de modificación del código fuente de las aplicaciones y de esta manera sigue siendo efectivo al momento de proteger los datos contra ataques dirigidos a cualquier vulnerabilidad.

Esta tecnología es relativamente nueva comparándola con los firewalls (Cortafuego), siempre WAF actúa delante de los servidores WEB y así se evita los ataques dirigidos a estos, WAF es diferente al usual Firewall. [15]

En la siguiente figura se muestra la situación deseada en el momento de la implementación de WAF.

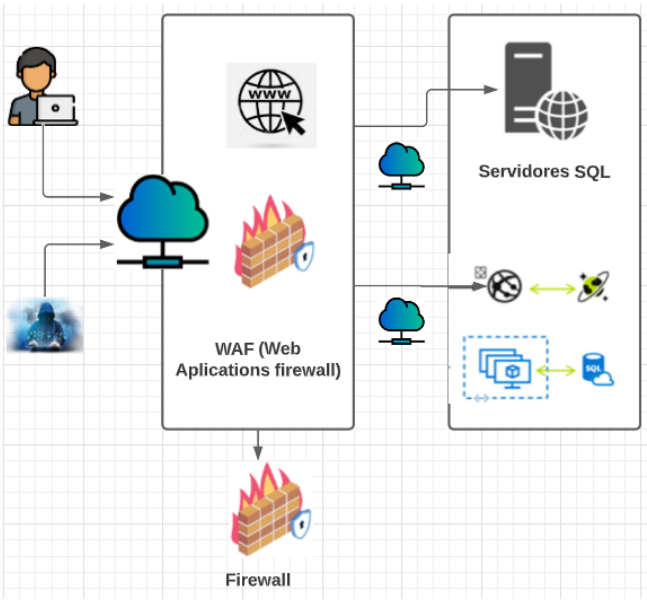

Figura 4. Modelo de uso WAF

WAF maneja varios modelos de implementación esto depende directamente de los servicios requeridos su plus es la flexibilidad y rendimiento en cualquier arquitectura, algunos de los módulos a implementar serían, instalación en la nube administrado como servicio, en instalación en la nube administración autogestionado, instalación en la nube administrado auto aprovisionado y WAF avanzado. [16]

2.7 INTRODUCCIÓN A LA SITUACIÓN DESEADA

La situación deseada esperada en prestar un servicio de consultoría enfocada a mostrar las virtudes de un WAF que permita fortalecer la seguridad de aplicaciones web , dicho servicio incluye entre otras cosas identificar actualmente cuales son las amenazas informáticas que diariamente intentan atacar las aplicaciones web con las que contamos y así mismo sugerir estrategias que permitan mitigar la intrusión de atacantes informáticos que puedan alterar los pilares de la seguridad de la información (Confidencialidad, Integridad y disponibilidad), la información de las amenazas actuales que afectan las aplicaciones web fue tomada de la página oficial de la OWASP [17]

Dicho servicio de consultoría está enfocado a empresas pymes de diferentes sectores lo que conlleva a evaluar diferentes escenarios para presentar el mejor servicio de consultoría de acuerdo con la necesidad tomando como referencia los pasos lógicos para una consultoría enfocada al sector TI [18]

SITUACIÓN ACTUAL

En la siguiente figura se muestra la situación actual que se tiene frente a la seguridad de las empresas pymes.

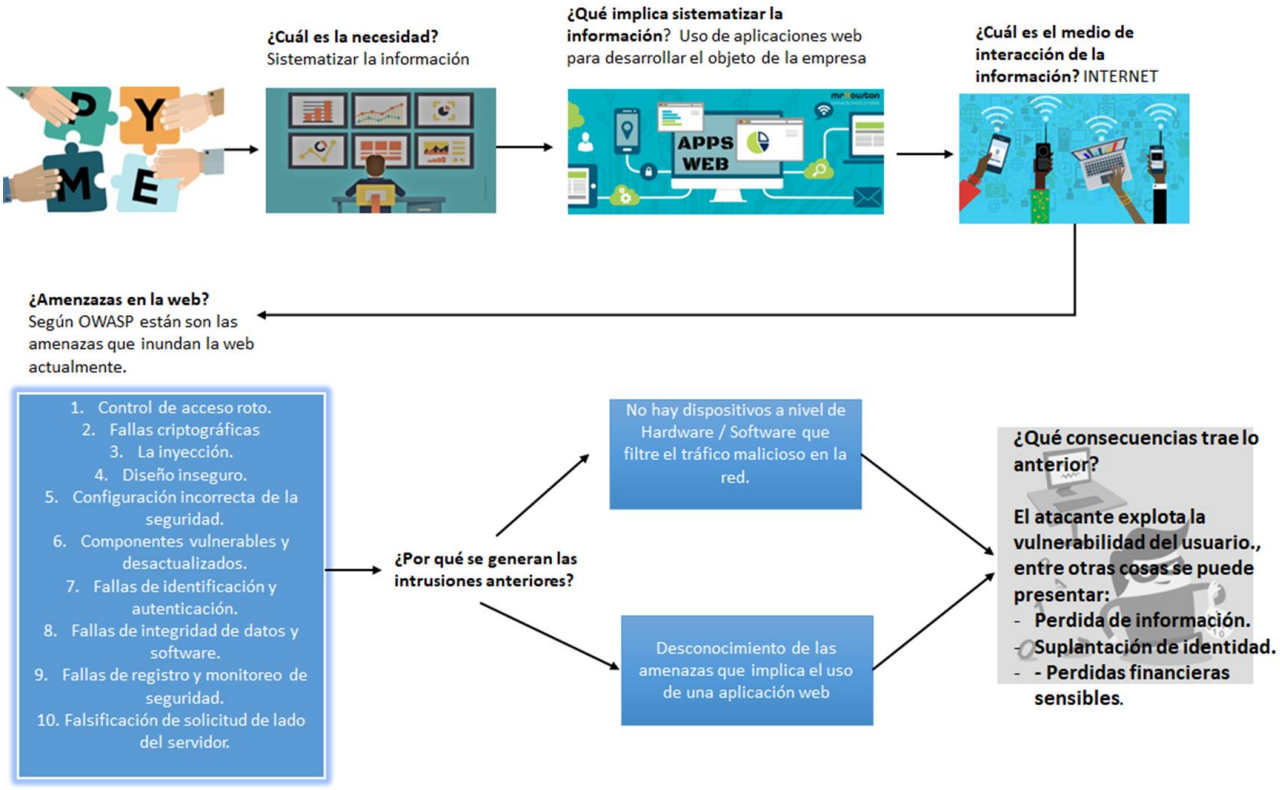

Figura 5. Situación actual Fuente Propia.

SITUACIÓN ESPERADA

En la siguiente figura se muestra la situación esperada al momento de hacer la asesoría y la implementación del servicio waf.

Figura 6. Situación esperada Fuente propia

2.8 PROPUESTA DE VALOR

Con nuestra solución de Web Application Firewall, puede tener la tranquilidad de que sus aplicaciones web están protegidas contra las amenazas en constante evolución del panorama de la seguridad cibernética, permitiéndote enfocarse en el crecimiento y el éxito de su negocio.

Protección avanzada para sus aplicaciones web: Nuestro WAF ofrece una defensa sólida y proactiva contra amenazas cibernéticas dirigidas a sus aplicaciones web. Utilizando tecnologías de vanguardia, nuestro WAF identifica y bloquea ataques como inyecciones SQL, cross-site scripting (XSS), ataques de fuerza bruta y más, asegurando que tus aplicaciones estén protegidas contra las vulnerabilidades más comunes.

Adaptabilidad a tus necesidades: Reconocemos que cada aplicación web es única, por lo que nuestro WAF se adapta a sus necesidades específicas. Podrá personalizar las reglas de seguridad, definir excepciones y ajustar la configuración para asegurarte de que la protección se alinee con los requisitos de su negocio, sin afectar negativamente el rendimiento de tus aplicaciones.

Monitoreo y análisis en tiempo real: Nuestro WAF proporciona monitoreo continuo y análisis en tiempo real de los intentos de ataques. Con un panel de control intuitivo, donde se podrá visualizar fácilmente los intentos de intrusión, analizar patrones de ataque y recibir alertas instantáneas cuando se detectan actividades sospechosas, lo que te permite tomar medidas rápidas para mitigar las amenazas.

Soporte técnico especializado: Nuestro equipo de soporte técnico altamente capacitado está listo para ayudar en cualquier momento. Ya sea que necesites asistencia en la configuración inicial, asesoramiento sobre mejores prácticas de seguridad o resolución de problemas, nuestro equipo estará a tu disposición para brindarte la ayuda necesaria y garantizar que obtengas el máximo valor de nuestro WAF.

Adicionalmente a las ventajas y beneficios de protección que ofrecemos también tenemos espacios destinados a nuestros clientes que nos ayudan a acercarnos más a ellos y mejorar su experiencia con nuestro servicio. Dentro de dichos espacios se destacan:

- Webinar con clientes y panel de expertos.
- Capacitaciones de Seguridad Informática.
- Demos de Servicios.

2.8.1 PERFIL DEL CLIENTE

Nuestros clientes potenciales serían las Pymes que operan aplicaciones web que implementen comercio electrónico y web propias debido a que son un objetivo común para los ataques cibernéticos.

Pymes de comercio electrónico y pymes que cuentan con su propia web. Las empresas que operan plataformas de comercio electrónico son un objetivo común para los ataques cibernéticos, ya que manejan grandes cantidades de información confidencial, como datos de tarjetas de crédito y detalles personales de los clientes.

Un WAF sería ideal para proteger sus aplicaciones web y salvaguardar la información confidencial de los usuarios.

Según estudios de ACOPI (Asociación Colombiana de las Micro, Pequeñas y Medianas Empresas), el 79,2 % de las pequeñas y medianas empresas en Colombia emplean redes sociales como apoyo tecnológico con fines comerciales, el 68,5 % cuentan con una página web particular y el 68,2 % usa la banca digital.[19]

2.8.2 MAPA DE VALOR

Se plantean los diferentes aspectos primordiales que se tendrán en cuenta para la identificación y optimización de la entrega de la solución propuesta.

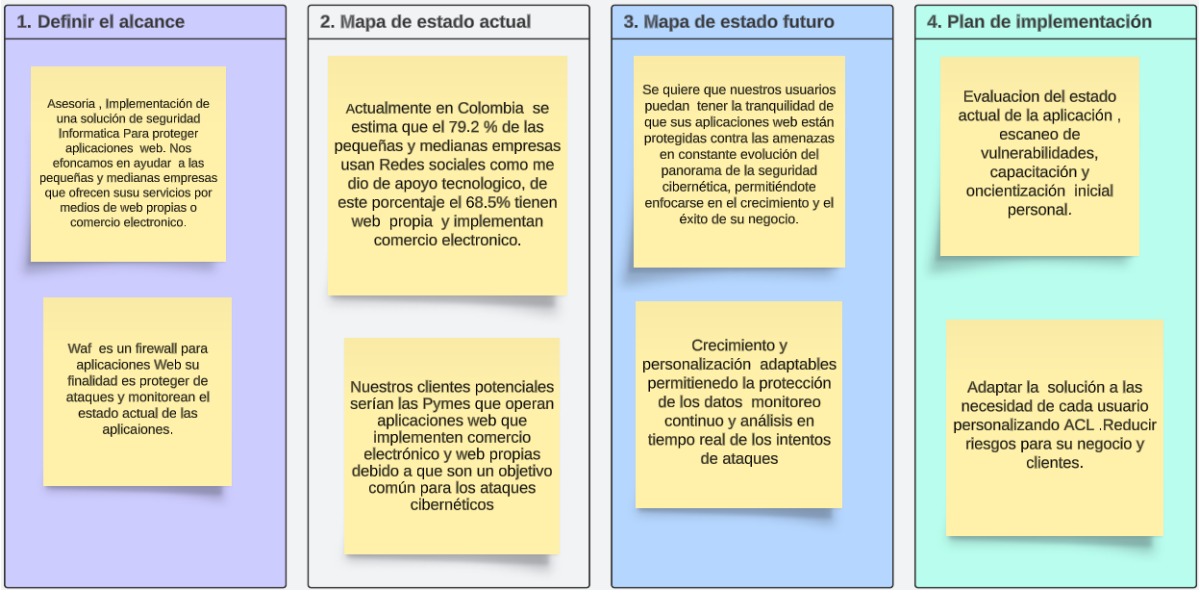

Figura 7. Mapa de valor Fuente Propia

3. ANÁLISIS DE LAS ALTERNATIVAS TÉCNICAS PARA SOLUCIONAR EL PROBLEMA

El mercado de los firewalls para aplicaciones web (WAF) es variado, tiene varias opciones de implementación que se soportan en los requisitos de la aplicación y seguridad de una empresa, actualmente existen tres tipos principales de WAF: basado en la nube, basado en Software y basado en Hardware a continuación se

ilustra en la tabla las ventajas y desventajas de cada uno en términos de coste, rendimiento, escalabilidad y mantenimiento:

	WAF Basado en la nube	WAF basado en Software	WAF basado en Hardware
Sugerido a:	**Empresas de cualquier tamaño (Grandes, medianas, pequeñas)**	**Empresas medianas y grandes**	**Empresas Grandes**
VENTAJAS	- Implementación sencilla. - inversión inicial mínima por parte del cliente - Nivel de protección constante, gestión centralizada - Suscripción del servicio basada en la seguridad como servicio(**SECaaS**). - Actualizaciones que son realizadas por el proveedor del servicio - mejor opción de implementación para entornos multi-cloud	- Opciones de personalización adicionales (esto teniendo en cuenta que se cuenten con los recursos y / o experiencia de seguridad a nivel interno de la empresa. - Costos iniciales de implementación y mantenimiento más económicos con respecto a una solución de WAF basado en Hardware	- Menor tiempo de latencia - Gran porcentaje de personalización por parte del cliente. - Espacio de ventilación en su totalidad
DESVENTAJAS	- Algunos sectores específicamente de gobierno y defensa están	- Implementación compleja - Depende de los recursos del servidor	- Inversión inicial costosa - Costos de mantenimie

	obligados a mantener toda la infraestructura y la data a nivel local lo que descarta la implementación WAF en la nube como una opción factible.	de aplicaciones para funcionar de manera correcta, no es elástico. - Las actualizaciones deben ser gestionadas por el cliente.	nto continuos - Costos operativos y de personal TI elevados - Actualizaciones y mantenimientos gestionados por el cliente

Tabla 2. Ventajas y desventajas de WAF basado en la nube, Hardware y Software Fuente Propia.

En la siguiente figura se muestra la arquitectura a nivel general de la solución Waf.

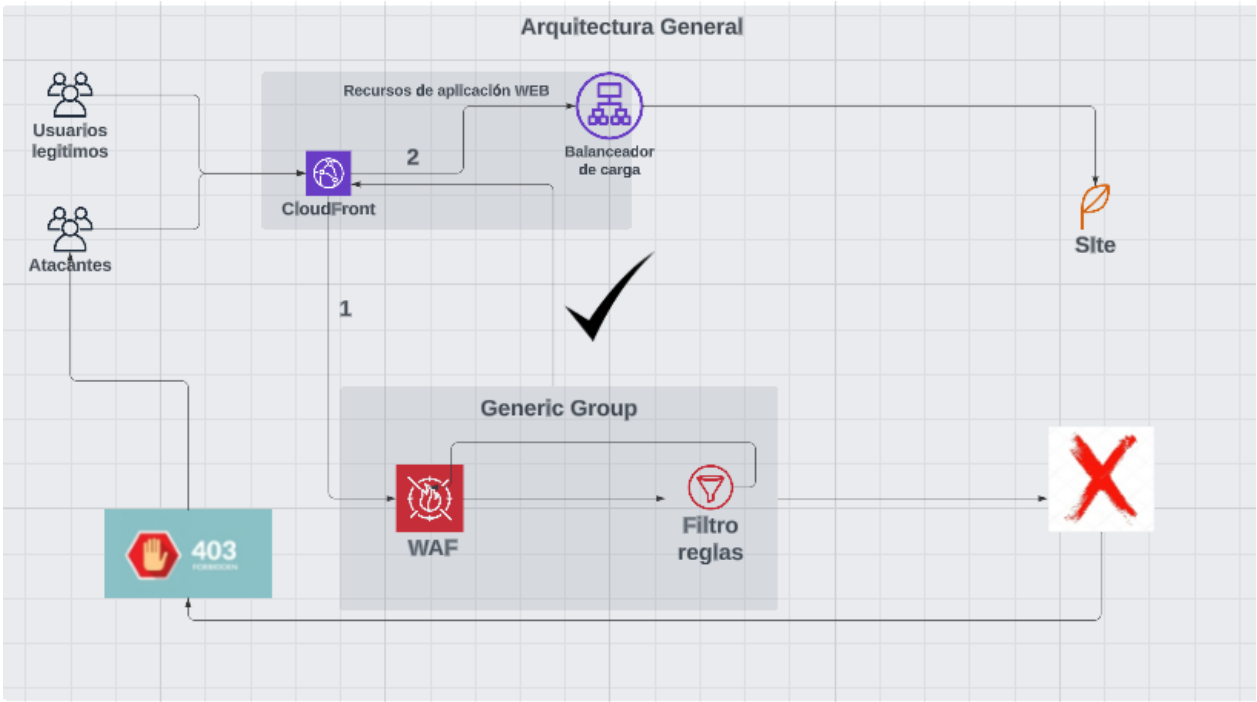

Figura 8. Arquitectura general WAF

Arquitectura general de la solución basada en un WAF basado en la nube.

La solución propuesta por nuestro servicio de consultoría e implementación con recursos con base en AWS ya que a nivel de mercado son económicos y solo se paga por el uso de los mismos con referencia a otros competidores, consiste en una arquitectura en donde hay dos caminos el primero consiste en que el atacante ingresa a través del cloudFront y de aquí es direccionado a la solución de WAF que tiene predeterminadas unas reglas que permiten identificar un ataque malicioso y así inmediatamente el sitio arroja un mensaje 403 que no permite que el ataque malicioso se lleve a cabo y la segunda ruta es a través de un usuario legítimo que se loguea y si no hay amenazas detectadas por el firewall el usuario legítimo accede al contenido de la página web.

La solución es variable de acuerdo a la necesidad que se identifique para el cliente.

Amazon CloudFront: servicio que se puede utilizar para entregar el sitio incluyendo el contenido estático, dinámico, streaming e interactivo de acuerdo a la necesidad del cliente.

Balanceador de carga: Distribuye de manera automática el tráfico de las aplicaciones entrantes entre varios destinos y dispositivos virtuales en una o varias zonas de disponibilidad (AZ)

En la siguiente figura se muestra la arquitectura propuesta con el fin de automatizar el proceso de detección de intrusiones y mediante un conjunto de reglas automatizadas permitir la denegación del servicio al intruso.

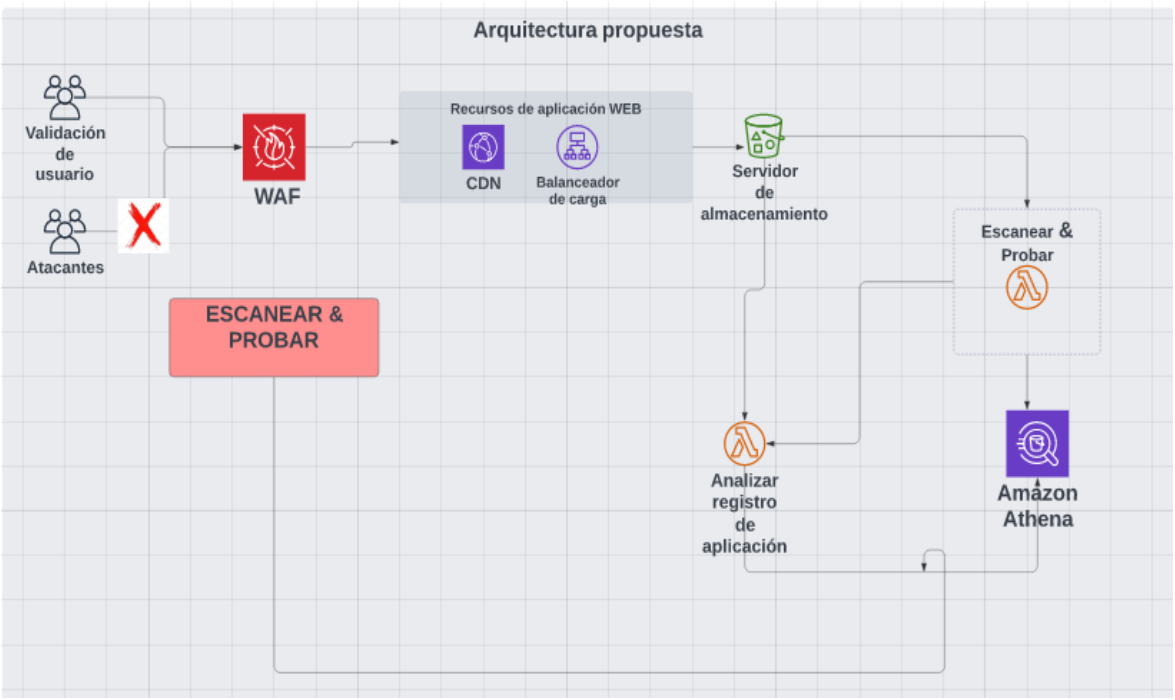

Figura 9. Solución arquitectura propuesta consultoría

¿Qué es un AWS WAF?

AWS WAF es un servicio de seguridad que le permite proteger sus aplicaciones y API web de los ataques comunes que pueden afectar su disponibilidad, seguridad o rendimiento. Se integra con los Application Load Balancers, los API Gateways y las distribuciones de AWS CloudFront, lo que facilita su implementación y administración, Se puede crear reglas personalizadas para filtrar el tráfico web según criterios como la dirección IP, el encabezado o el cuerpo HTTP, el URI personalizado o el comportamiento del usuario. También puede utilizar reglas administradas que le proporcionan protecciones preconfiguradas contra bots maliciosos, inyección SQL, cross-site scripting (XSS), inundaciones de HTTP y ataques de atacantes conocidos.

Ofrece una gran flexibilidad y control para definir las condiciones que desea bloquear o permitir. Además, puede utilizar las API de AWS WAF para automatizar la creación y el mantenimiento de las reglas, así como para integrarlas en su proceso de desarrollo y diseño. También ofrece una visibilidad detallada del tráfico web y las métricas de seguridad, lo que ayuda a monitorizar y analizar el comportamiento de sus aplicaciones y API web.

4. MODELO DE NEGOCIO

El modelo de negocio se trabajó bajo el marco de canvas donde muestra los pilares fundamentales para hacer viable el proyecto

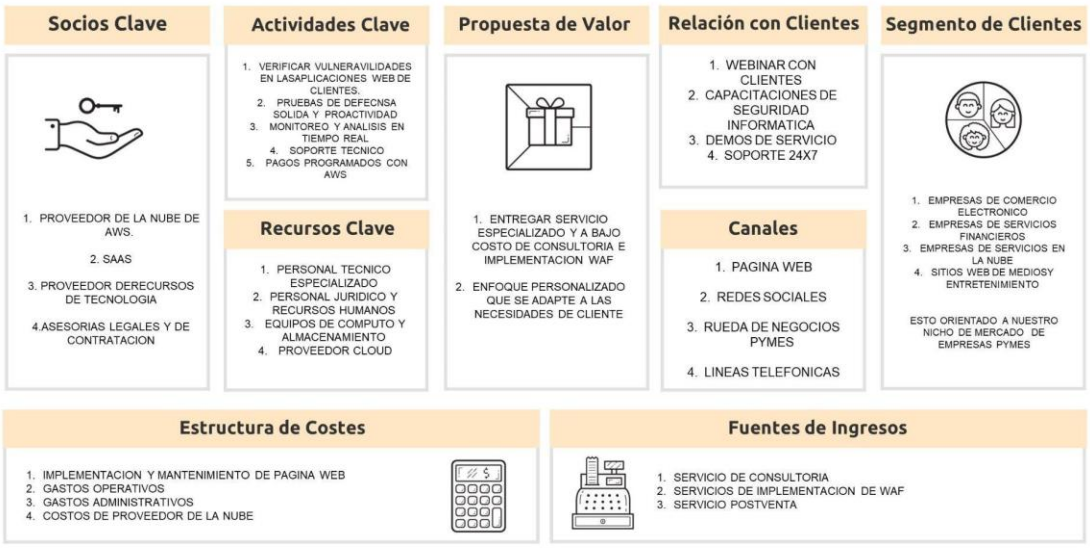

Figura 10. Modelo de Negocio

4.1 PROPUESTA DE MODELO DE NEGOCIO

Este modelo de negocio se enfoca en ofrecer servicios de implementación y asesoría en WAF a empresas que requieren una mayor seguridad en sus aplicaciones web. El objetivo es brindar a las empresas una solución completa que les permita:

- Proteger sus aplicaciones web de posibles ataques y vulnerabilidades.
- Reducir riesgos para su negocio y clientes.
- Mejorar la disponibilidad y rendimiento de sus aplicaciones.

Para lograr estos objetivos, la propuesta de servicio consiste en lo siguiente:

- Servicio de evaluación de vulnerabilidades: Este servicio implica llevar a cabo un estudio detallado de las aplicaciones web de la empresa para identificar posibles vulnerabilidades y brechas de seguridad. Es un paso crítico y necesario antes de la implementación de un WAF.

- Servicio de implementación de WAF: Una vez identificadas las vulnerabilidades, el siguiente paso es la implementación de un WAF. Para ello se debe seleccionar la solución WAF adecuada, y proceder con su configuración y puesta en marcha.

- Servicio de monitoreo y mantenimiento: Una vez implementado el WAF, se debe llevar a cabo un monitoreo continuo de las aplicaciones web para detectar posibles incidentes de seguridad y vulnerabilidades, así como para realizar ajustes y mejoras al WAF.

- Servicio de asesoramiento: Además de los servicios de implementación y mantenimiento, es importante brindar asesoramiento a las empresas para que puedan entender y mejorar su nivel de seguridad en aplicaciones web. Este servicio debe incluir recomendaciones para optimizar la seguridad de las aplicaciones web.

Este modelo de negocio ofrece varios beneficios a las empresas que buscan una mejor seguridad para sus aplicaciones web. Estos beneficios incluyen:

- Reducción de riesgos y costos: Al implementar un WAF, se minimizan los riesgos y costos asociados con los ataques y vulnerabilidades.

- Mejora del rendimiento: Con un WAF implementado, las aplicaciones web tienen un rendimiento mejorado y mayor disponibilidad.

- Expertos en seguridad: Este modelo de negocio tiene como objetivo brindar un equipo de expertos en seguridad para brindar un servicio de calidad.

El servicio incluye el diseño, la instalación, la configuración, el mantenimiento y el monitoreo de un waf que se adapte a las necesidades y requerimientos de cada cliente. El servicio de implementación y asesoría de waf se basa en las siguientes ventajas competitivas:

- Experiencia y conocimiento técnico en el ámbito de la seguridad informática y las aplicaciones web.
- Uso de herramientas y metodologías reconocidas y actualizadas para el análisis, el diagnóstico y la solución de problemas.

- Atención personalizada y adaptada a las características y expectativas de cada cliente.
- Seguimiento continuo y reportes periódicos del estado y funcionamiento del waf.
- Soporte técnico permanente y asistencia en caso de emergencias o incidencias.
- Precios competitivos y flexibles según el tamaño, la complejidad y el nivel de seguridad requerido por cada aplicación web.

4.2 VALIDACIÓN DEL MODELO DE NEGOCIO

Para la validación el negocio la propuesta se basa en un modelo de encuestas con ellos para realizar un reconocimiento de la demanda, realizar encuestas, entrevistas con nuestros posibles clientes para obtener retroalimentación sobre el modelo de negocio propuesto. Realizando preguntas como su interés en contratar servicios de implementación de WAF, las preocupaciones de seguridad web y si estarían dispuestos a pagar por este tipo de servicio.

También realizar implementaciones piloto de WAF en un número pequeño de clientes seleccionados. Monitoreando y evaluando los resultados, tanto en términos de rendimiento de la solución como de la satisfacción del cliente. Se utilizará esta información para sacar oportunidades de mejorar y ajustar el modelo de negocio antes de escalar a un nivel más amplio y salir a producción. El modelo de negocio es un proceso por etapas que requiere adaptación constante. Hay que escuchar a los clientes y mantenerse actualizado con las tendencias y avances en seguridad web para asegurar el éxito a largo plazo del negocio.

5. PROPUESTA DE LA SOLUCIÓN TECNOLÓGICA

Con base a la información con la que actualmente contamos, la cual se ha descrito en los puntos anteriores, el presente proyecto contiene un proceso de transformación y actualización tecnológica el cual podemos decir que va por el camino adecuado.

La solución tecnológica que se propone para la implementación y asesoramiento de WAF es la siguiente:

Evaluación de la infraestructura: En primer lugar, se realizará una evaluación de la infraestructura tecnológica actual de su empresa para determinar la mejor solución WAF. Se analizará aspectos como las aplicaciones web a proteger, el tráfico generado, los recursos disponibles, entre otros.

Selección de la solución WAF: Una vez evaluada la infraestructura, se selecciona la solución WAF más adecuada para su empresa. Se asegurará de que se ajuste a sus necesidades y presupuesto.

Instalación y configuración del WAF: El personal técnico especialista instalará y configurará la solución WAF seleccionada. Se ajustarán los parámetros necesarios para crear una política de seguridad adecuada y personalizada.

Análisis de vulnerabilidades: Se realizará un análisis de vulnerabilidades en sus aplicaciones web para descubrir debilidades y posibles puntos de entrada que puedan ser explotados por ataques malintencionados.

Monitoreo y gestión de alertas: Se configurarán las herramientas de monitoreo que permitan mantener vigilada su infraestructura en tiempo real. Las alertas que se generen serán gestionadas por nuestros técnicos especializados.

Soporte y asesoramiento: El equipo de soporte técnico y expertos en seguridad estarán disponibles para brindarle el asesoramiento necesario en caso de surgir nuevos incidentes de seguridad, Con la solución tecnológica, se garantizará la tranquilidad de tener una solución WAF configurada y monitoreada por expertos en seguridad informática. Se asegurará la protección de la infraestructura y sus aplicaciones web, minimizando el riesgo de sufrir ataques malintencionados.

6. ANÁLISIS DEL PROCESO DE TRANSFORMACIÓN DIGITAL

El proceso de transformación digital en Colombia ha tenido un fuerte crecimiento en los últimos años, situación reforzada por la necesidad de las empresas de seguir funcionando a pesar de los efectos causados por la pandemia ya que fue un evento inesperado que obligó acelerar dicho proceso de transformación digital que permitiera a las Pymes adaptarse a esta situación de la cual no había manera de anticipar.

En este nuevo mercado competitivo y a nivel global es necesario que las empresas sean redefinidas para que a través de procesos de transformación digital entre otras cosas estén en la capacidad de mejorar su rendimiento en los procesos que ellas desarrollan.

Digitalizar la empresa es una tarea compleja que requiere tener una secuencia de pasos para lograr el objetivo porque implica diseñar procesos que antes funcionaban pero que ahora pueden ser lentos en este objetivo de automatizar, lo anterior también aplica para productos, servicios, relaciones con proveedores ya que también hay que incluirlos en este proceso de transformación y sobre todo con el modelo de negocio de la Pyme. Para llevar a cabo esta transformación se requiere de un cambio organizacional en el que se debe trabajar mucho el tema de incluir a los trabajadores en este proceso de adaptación a las necesidades del cliente con base a el uso de distintas tecnologías en auge que permitan automatizar procesos y hacer que la Pyme se centra en generar valor y uso de recursos en decisiones estratégicas que generen un plus. Para que lo anterior funcione como una sinergia es clave el liderazgo que inyecte la dirección para este proceso de transformación digital.

Objetivos de desarrollo Sostenible

El 25 de septiembre de 2015, los líderes mundiales adoptaron un conjunto de objetivos globales para erradicar la pobreza, proteger el planeta y asegurar la prosperidad para todos como parte de una nueva agenda de desarrollo sostenible. Cada objetivo tiene metas específicas que deben alcanzarse en los próximos 15 años.

Para alcanzar estas metas, todo el mundo tiene que hacer su parte: los gobiernos, el sector privado, la sociedad civil y **personas como usted**.

¿Quieres participar? Puedes empezar por decirle a todos acerca de estos objetivos.[20]

Figura 11. Objetivos de desarrollo sostenible Fuente UNICEF

De lo anterior nuestro proyecto de consultoría e implementación de un WAF quiere contribuir en el objetivo de desarrollo sostenible número 9 **Industria, Innovación e Infraestructuras** haciendo énfasis en el numeral **9.b Apoyar el desarrollo de tecnologías, la investigación y la innovación nacionales en los países en desarrollo,** incluso garantizando un entorno normativo propicio a la diversificación industrial y la adición de valor a los productos básicos, entre otras cosas

A través de nuestra solución de consultoría e implementación de un WAF a cada uno de nuestros clientes estamos contribuyendo con el apoyo al desarrollo de las tecnologías , la manera de hacerlo es identificando a nivel de seguridad las falencias de las aplicaciones web que usan nuestro clientes y mediante tecnologías a un costo accesible para ellos brindar un acompañamiento que incluye la asesoría con el fin de que el cliente entienda la importancia de adquirir una solución que le permita reforzar la seguridad de su información.

ASPECTOS LEGALES Y CONTRATACIÓN

Como proveedores de servicios el compromiso es a realizar la Asesoría e implementación de la solución WAF de acuerdo con la propuesta y revisión que se genere con cada cliente, los contratos se ejecutarán a través de órdenes de trabajo bajo la modalidad de proyectos donde se especifiquen objetivos y los entregables para cada proyecto. Como proveedores de servicios se debe adquirir el compromiso a que los servicios prestados cumplan con todas las especificaciones técnicas solicitadas por el usuario final , para este caso se deben definir dichas especificaciones en la preparación de los requerimientos técnicos previos acordados entre las partes, se entiende que los clientes no son expertos en esta clase servicios, por ello como proveedor y desde el conocimiento y experiencia, es obligatorio realizar todas aquellas tareas, obras, actividades y acciones que técnicamente correspondan a esta clase de servicio y que se acuerden en cada orden de trabajo.

Dentro de las obligaciones contractuales se tendrán las siguientes:

- Asegurar la competencia y disponibilidad del personal adecuado para la prestación de los servicios pactados en el contrato de acuerdo a lo establecido en la propuesta y alcance técnico.
- Cumplir con la normatividad, protocolos y estándares de seguridad y privacidad del manejo de la información según lo establecido en la LEY 1273. 2009 de la protección de la información y de los datos.
- Asegurar el manejo adecuado del personal asignado para el cumplimiento de los servicios.
- Mantener la arquitectura de las aplicaciones para la prestación de los servicios según lo acordado con el usuario final, de ser necesario algún tipo de cambio debe ser notificado con anterioridad.
- Asegurar que se realice una gestión adecuada de riesgos sobre los servicios prestados por los usuarios sin afectar a terceros.
- Entrega de documentación y transferencia de conocimiento para los temas de mantenimiento y apoyo de los servicios luego del inicio del contrato.

Algunas de las obligaciones de los usuarios serán:

- Colabora con el proveedor en lo que esté dentro de su alcance para que se lleve en buenos términos y a cabalidad lo pactado, esto no quiere decir que deban revelar de alguna función al proveedor.
- Pagar el valor estipulado en los servicios contratados bajo los términos establecidos.

- Coordinar en común acuerdo cualquier modificación o implementación que quieran generar sobres lo ya establecido.

Para aspectos legales validamos ley vigente es la 1978 DE 2019 que con la cual se actualizó y se modernizó la Ley 1341 2009 donde el artículo 3 nos habla de la prioridad al acceso y uso de las tecnologías de información.

“El estado y en general todos los agentes del sector de las Tecnologías de la Información y las Comunicaciones deberán colaborar, dentro del marco de sus obligaciones, para priorizar el acceso y uso a las Tecnologías de la Información y las Comunicaciones en la producción de bienes y servicios, en condiciones no discriminatorias en la conectividad. la educación, los contenidos y la competitividad”. Esto va de la mano con el crecimiento de la digitalización de los negocios y transacciones en la red.

También al ser un servicio que involucra computación en la nube se debe tener en cuenta el documento guía publicado por el MINTIC (Ministerio de Tecnologías de la Información y las Comunicaciones) donde se establecen criterios y definiciones par saber si una persona natural o jurídica es un prestador de servicios de computación en la nube, a su vez expone que se debe tener en cuenta en la contratación de estos servicios. En Colombia se garantiza que uno de los principios de las Tecnologías de la información es la neutralidad que ella debe tener cuyo concepto fue definido en la Ley de TIC 1341 del 30 de Julio de 2009 y se ratifica en el decreto 1078 de 2017 artículo 2.2.9.1.1.1 de la estrategia de Gobierno en Línea (GEL).[21]

CONCLUSIONES

En conclusión, la asesoría e implementación de un WAF (web application firewall) es una solución eficaz y rentable para proteger las aplicaciones web de los ataques cibernéticos. Un WAF permite filtrar el tráfico entrante y bloquear las solicitudes maliciosas que intentan explotar las vulnerabilidades de las aplicaciones.

Además, un WAF ofrece beneficios como el cumplimiento de las normativas de seguridad, la mejora del rendimiento de las aplicaciones y la reducción de los costos operativos. Por lo tanto, Se puede concluir que es viable la entregar estos servicios a una empresa donde sabe que se contará con el respaldo de un área especializada en WAF que pueda brindar una asesoría personalizada y una implementación adecuada según las necesidades y objetivos de cada cliente.

La implementación de un WAF (Web Application Firewall) es esencial para garantizar la seguridad de cualquier aplicación web. Un WAF ayuda a proteger contra una amplia gama de ataques, tales como inyecciones SQL, XSS y CSRF, entre otros. Además, ofrece una capa adicional de defensa para complementar las medidas de seguridad estándar de la aplicación web.

La implementación de un WAF se ha vuelto fundamental en la protección de las aplicaciones web contra amenazas y ataques cibernéticos cada vez más sofisticados. Es crucial reconocer la importancia de la seguridad web y la necesidad de contar con soluciones efectivas para salvaguardar la integridad y confidencialidad de los datos.

REFERENCIAS

[1] Cámara Colombiana de Informática y Telecomunicaiones, «Hurto a través de medios y sistemas informáticos siguen creciendo en Colombia,» *https://www.ccit.org.co/,* 2022.

[2] Imperva, «imperva.com,» Imperva, 02 2022. [En línea]. Available: https://www.imperva.com/resources/resource-library/reports/kuppingercole-leadership-compass-web-application-firewalls-2022-full-report/. [Último acceso: 05 11 2022].

[3] F5, «F5.com,» F5, 01 2022. [En línea]. Available: https://www.f5.com/pdf/solution-overview/f5-big-ip-advanced-waf-protection-for-every-app-anywhere.pdf. [Último acceso: 01 11 2022].

[4] O. Foundation, «owasp,» OWASP Foundation, [En línea]. Available: https://owasp.org/www-project-top-ten/. [Último acceso: viernes Octubre 2022].

[5] colombiaproductiva, «Colombia Productiva,» Colombia Productiva, 5 10 2019. [En línea]. Available: https://www.colombiaproductiva.com/ptp-capacita/publicaciones/pactos-por-el-crecimiento/pacto-por-el-crecimiento-y-para-la-generacion-10/infografia-software-29-11.. [Último acceso: 9 10 2022].

[6] colombiaproductiva, «Colombia Productiva,» Colombia Productiva, 5 10 2019. [En línea]. Available: https://www.colombiaproductiva.com/ptp-capacita/publicaciones/pactos-por-el-crecimiento/pacto-por-el-crecimiento-y-para-la-generacion-10/infografia-software-29-11.. [Último acceso: 9 10 2022].

[7] dian.gov,» DIAN, 12 2020. [En línea]. Available: https://www.dian.gov.co/normatividad/Normatividad/Resoluci%C3%B3n%20000114%20de%2021-12-2020.pdf. [Último acceso: 11 2022].

[8] Dian, «Dian.gov,» DIAN, 12 2020. [En línea]. Available: https://www.dian.gov.co/Prensa/Aprendelo-en-un-DIAN-X3/Paginas/Abece-Actividad-Economica-para-la-Industria.aspx. [Último acceso: 30 10 2022].

[9] Doreen Bogdan-Martin,, «itu,» itu, 2022. [En línea]. Available: Available: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E. [Último acceso: 28 10 2022].

[10] Doreen Bogdan-Martin,, «itu,» itu, 2022. [En línea]. Available: Available: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E. [Último acceso: 28 10 2022].

[11] Steve Morgan, «https://cybersecurityventures.com/,» 2022. [En línea]. Available: https://cybersecurityventures.com/cybersecurity-almanac-2022/. [Último acceso: 07 Noviembre 2022].

[12] https://www.larepublica.co/empresas/condiciones-del-mercado-de-ciberseguridad-colombiano-atraen-a-nuevos-jugadores-3324669. (17 de Marzo de 2022). Condiciones del mercado de ciberseguridad colombiano atraen a nuevos jugadores. Diario La República.

[13] https://www.ccit.org.co/noticias/crecieron-28-las-denuncias-de-ciberataques-a-redes-de-telecomunicaciones/. (2020). Más de 54.000 denuncias de ciberdelitos se registraron a cierre del tercer trimestre de 2022. Cámara Colombiana de Informatica Y telecomunicaciones.

[14] Camara de Comercio de Bogota. (2023). Empresas renovadas. *Camara de Comercio Bogotá*, https://www.ccb.org.co/observatorio/Dinamica-Empresarial/Dinamica-empresarial/EMPRESAS-RENOVADAS-Las-MiPymes-representan-el-99-3-de-las-empresas-renovadas-y-las-micro-y-pequenas-el-97-7#:~:text=En%20enero%20de%202023%20en,de%2010.501%20a%2012.879%20empres.

[15] Hoffman, Karen Scarfone - Paul, «NIST,» National Institute of Standars and Technology, 09 2020. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf. [Último acceso: 04 11 2022].

[16] F5, «F5.com,» F5, 2022. [En línea]. Available: f5.com/es_es/services/resources/glossary/web-application-firewall. [Último acceso: 4 11 2022].

[17] L. Mendiola, «Artek,» 18 10 2021. [En línea]. Available: https://artek.edu.mx/noticia_eventos/los-tres-pilares-de-la-ciberseguridad/. [Último acceso: 25 Octubre 2022].

[18] O. FOUNDATION, «OWASP ORG,» 2021. [En línea]. Available: https://owasp.org/www-project-top-ten/. [Último acceso: 06 NOVIEMBRE 2022].

[19] DIGITALIZACIÓN ACOPI Y DESARROLLO SOSTENIBLE DE LA MYPIME EN COLOMBIA,» ESTUDIOS ECONÓMICOS ACOPI, p. 24, 2022.

[20] UNICEF. (2023). Objetivo 9: Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación. Objetivos de Desarrollo Sostenible. https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible.

[21] Ministerio de Tecnologías de la Información y las Comunicaciones, «Guia Consulta Publica Computación en la Nube,» https://normograma.mintic.gov.co/mintic/docs/directiva_documento_0002_2018.htm, p. 35, 2017.

LISTA DE FIGURAS

LISTA DE TABLAS